Defense Advanced Research Projects Agency (DARPA)
Information Resources Directorate (IRD)

Attachment No. 10

Incumbent Contractor's Statement of Work (SOW)

Defense Advanced Research Projects Agency (DARPA)
Information Technology Services
Section C - Statement of Work

Table of Contents:

Attachments:

1 Presentation dated July 7, 2000 and Narrative Description (draft) dated 11/3/00 of DARPA's information technology strategic direction and operational objectives

2 Current DARPA seat types, network and telecommunications services and configurations

3 Service Level Agreements

4 Smart Card Reader Requirements

5 DARPA Y2K Plan

6 Incumbent Contractor's Statement of Work

7 Current Projects being performed by Incumbent Contractor

Task Order Title: Information Technology Services for the Defense Advanced Research Projects Agency (DARPA)

Task Order Number: *To be assigned*

Fiscal Years: 1 year base (FY01) with 4 option years (FY 02 – 04)

ITOP Functional Area: Systems Operations and Management (SOM)

1.0 Introduction

This is a statement of work for information technology seats and services for the Defense Advanced Research Projects Agency (DARPA). DARPA is located at 3701 North Fairfax Drive, Arlington, VA 22203-1714 and in other buildings nearby. The DARPA mission is to maintain U.S. technological superiority over potential adversaries by identifying and supporting breakthrough technologies of interest to the military. Information technology services in support of this responsibility require state-of-the-art tools and services, and rapid, flexible response to mission essential and evolving customer requirements. Attachment 1 contains a presentation and narrative description of DARPA's information technology strategic direction and operational objectives, which are expected to evolve over the course of this task order. The Information Resources Division (IRD) of DARPA will manage this task order. In accordance with H. 23, EXCLUSION FROM FUTURE GOVERNMENT CONTRACTS, the Contractor is notified that there are situations under this Task Order that would permit the provisions of this special contract requirement to apply. The contractor shall during the period of performance of this contract and for one year after, be excluded from competition for, and award of, any other contractual arrangements as prime contractor, subcontractor, partner, or in any other capacity for the Defense Advanced Research Projects Agency without the express written approval of the Contracting Officer. Some or all of the contractor's employees may or shall be required to submit the Non-Disclosure Agreement included as Attachment J-8 of the basic contract. The intent of this provision to prevent a situation in which a company who has unlimited access to DARPA information (acquisition, budget, project plans, etc.) is able to bid on future DARPA work where information regarding that work would provide an unfair competitive advantage. Offerors who may have a potential conflict of interest under this clause should request a review by the contracting officer. Requests for such reviews should be submitted to the contracting officer in writing and include: Name of company, current DARPA contract number, role of the contractor (prime or sub), nature of the work performed, and a description of the current level of access to DARPA facilities and information.

1.1 Background

For the past 15 years information technology service in support of DARPA's mission requirements has been provided in accordance with a government-owned contractor-operated (GOCO) model. Hardware, software, network infrastructure components and telecommunications services have been purchased from vendors directly by DARPA and are government-owned. DARPA has obtained information technology support services through competitively-awarded small business set-aside cost-plus fixed fee contracts with Computing Analysis Corporation (CAC). The statement of work for the

incumbent contractor (CAC) is provided as Attachment 6. Attachment 7 is a list of projects currently being performed by the incumbent contractor. DARPA mission requirements for information technology service have outgrown and outpaced the current GOCO model. In order to respond more effectively and efficiently to mission requirements, DARPA seeks to move toward an information technology managed services model to include provision of all seat types, network and telecommunications infrastructures and related services necessary to meet known mission requirements, augmented with COTS and Expert Assistance catalogs that permit the ordering of items and labor to meet unplanned and emerging mission requirements. DARPA will transition management and ownership of all government-owned assets to the successful contractor. The incumbent services contractor is working under a full performance contract option that expires on 4 March 2001. Although one full performance option year remains in the incumbent service contractor's current contract, DARPA plans to award the base year task under this contract to commence in mid-March 2001. To effect transition from the incumbent to the successful offeror, DARPA will award a contract option to the incumbent to transition to the successful offeror. Attachment 2 contains a listing of all current DARPA seat types, network and telecommunications services and configurations supported by the incumbent. DARPA provides government-furnished space for the incumbent as follows: 8400 square feet at 3701 North Fairfax Drive, 6000 square feet at 3803 North Fairfax Drive, and 2220 square feet at 3601 North Fairfax Drive. DARPA will continue to provide government-furnished space to the successful offeror and will transition occupancy of space currently occupied by the incumbent.

2.0 Objectives

DARPA envisions that the successful offeror will provide and manage the full range of information technology service, support, and infrastructure necessary to implement the DARPA information technology strategic direction and operational objectives contained in Attachment 1, which are expected to evolve over the course of this task order. DARPA seeks to free the government staff from day-to-day project management and implementation of information technology services described in the statement of work by outsourcing those to the successful offeror. DARPA envisions that the government staff will focus on inherently governmental functions to include articulating mission requirements to the contractor, strategic planning, capital planning, independent verification and validation, and performance monitoring. DARPA may use other government or commercial third parties to advise and/or assist in performing its responsibilities.

Information Technology services provided under this statement work are essential to the accomplishment of DARPA's mission. DARPA has been and expects to be in the foreseeable future, a multi-platform environment. It is critical that continuity of operations and services be maintained at the current full performance level during the period of transition from the incumbent contractor to the successful offeror. To minimize the risk inherent in transition DARPA will proactively facilitate the transfer of explicit and tacit knowledge, methods, and procedures from the DARPA staff and the incumbent contractor staff to the successful offeror. The provisions of FAR 52.237-3(c) apply. To create an environment for successful transition, DARPA envisions that this statement of work will be accomplished in a manner that provides an orderly 'ramp up' for the successful offeror and an orderly 'ramp down' for the incumbent contractor.

3.0 Scope

This Statement of Work establishes the basic requirements related to providing general office

computing, networking, and communications service and technical support to DARPA. This statement of work consists of the following sections:

1. Service Delivery Points (includes seat types)
2. Customer Information Technology (IT) Services
3. Information Assurance(IA)/Computer Network Defense (CNO) Services
4. Catalog Services
5. Transition Services

Work identified in this document shall meet the levels of service specified in Attachment 3, Service Level Agreements (SLAs). Where unpriced options are exercised by DARPA, their accompanying description of services will be developed using the SLAs contained in Attachment 3 as the entering baseline. The resulting description of services will include any additions or changes to accommodate additional or customer-specific requirements.

4.0 Definitions

For the purposes of this document, the following definitions apply:

Assurance refers to availability, restricted access/confidentiality, integrity/data quality, attack/intrusion detection time, and attack termination time.

Capacity refers to ubiquity of access, connectivity, redundancy/diversity, compute capacity, committed information rate/peak information rate, and growth potential/scalability.

Customer Survey is the means used to measure the quality and timeliness of a delivered service.

E-Mail refers to a widely used Network application in which mail messages are transmitted electronically between end users over various types of networks using a variety of network protocols. An electronic means for communication in which (a) usually text is transmitted, (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee.

Legacy System refers to a hardware and/or software system that consists in whole (or part) of legacy applications, or uses legacy applications to achieve its transport or enabling capability.

Legacy Application refers to a software program developed or tailored specifically for use on an internal DARPA network.

Medium Grade Service (MGS) is a managed set of Commercial Off-The-Shelf (COTS) e-mail products that utilize the DoD Medium Assurance Public Key Infrastructure (PKI). As a subset of the Defense Message System (DMS), MGS represents a set of Internet standards agreed upon by government and industry. It uses Simple Mail Transfer Protocol (SMTP) for messaging services, Lightweight Directory Access Protocol (LDAP) for directory services, Secure Multipurpose Internet Mail Extension (S/MIME) for data encryption and digital signatures, and PKI certificates for individual identity. MGS will provide secure, interoperable messaging in an open, multi-vendor environment.

Responsiveness refers to latency, throughput, training, interoperability, customer service, adaptability to stress, restoration time, time to increase/enhance capability, and technical refresh rate.

Seamless refers to the ability to function effectively without loss of capability.

Service Level Agreement (SLA) is a specified level of service included as part of the statement of work as Attachment 3.

User Account refers to authorized access to the specified service exclusive of the hardware and LAN drop. User accounts will be aggregated at the enterprise level for billing purposes.

5.0 Statement of Work

5.1 DARPA Service Delivery Points (SDPs)

The contractor shall provide services with security features to a range of end points that include data, video conferencing center, printer and wireless seats; the general DARPA enterprise infrastructure, and external networks for interface with commercial and other Department of Defense (DoD) communications environments. The contractor shall provide support for DARPA Service Delivery Points headquartered at 3701, 3801, 3803, 3811, and4001 North Fairfax Drive, Arlington, VA that are existing users of those services. (Note: Support at 3811 North Fairfax Drive does not include the following services: data cabling, and network infrastructure. Network services for SDP located at 3811 North Fairfax Drive to the DMSS will be available through Virtual Private Networking (VPN) connection)

A service delivery point comprises the hardware, software, and security features (e.g. smart card technology) necessary for DARPA users to perform computing functions, to access computing resources and to receive the Customer Information Technology services described in section 5.2 of this SOW. Data Seat Service Delivery Points configurations (hardware and software) are proposed by the vendor and reviewed and approved in accordance with the Configuration Control Board (CCB) defined in section 5.2 of the SOW

5.1.1 Data Seats

A data seat is comprised of the hardware, software, security features and services provided to DARPA users as computing resources. The data seats are defined as follows:

A. Unclassified Data Seats SDPs

1.

1. Fixed Data Seat (Fixed SDP (either desktop or tower configuration) which includes the standard hardware and software configuration and is capable of performing local and network computing functions with access to the DARPA Management Services System (DMSS));
2. Portable Data Seat (Portable SDP (Notebook, Laptop, or Tablet PC) which includes the standard hardware and software configuration which may be used to access the DMSS. The portable data seat includes docking station or port replicator technology capable of connecting alternative input

(i.e. keyboard, mouse) and output (i.e. monitor) devices. The Portable Data Seat has additional features which provide for remote access to DMSS services as stated in section 5.2.1.15);

3. Remote Data Seat (SDP located outside the DARPA enclave with remote connectivity to the DMSS);

4. Hybrid Fixed Data Seat (Fixed Data Seat (A.1. above), which includes non-standard software or hardware);
5. Hybrid Portable Data Seat (Portable Data Seat (A.2. above), which includes non-standard software or hardware); and
6. Multiple Use Data Seat (User Service Account which provides access to the DMSS, Customer IT Services for personnel (i.e. Department of Defense (DoD) government employees, contractors, or specified liaisons) who do not require a data seat for their exclusive use).

B. Classified Data Seats SDPs

1. Fixed Data Seat (Fixed SDP (either desktop or tower configuration) which includes the standard hardware and software configuration, is capable of performing local and network computing functions, and with no connectivity to the DMSS, but which may be connected to an internal or external classified network. This seat includes classified seat services);

2. Portable Data Seat (Portable SDP (Notebook, Laptop, or Tablet PC) which includes the standard hardware and software configuration, is capable of performing local and network computing functions, and with no connectivity to the DMSS, but which may be connected to an internal or external classified network. The portable data seat includes docking station or port replicator technology capable of connecting alternative input (i.e. keyboard, mouse) and output (i.e. monitor) devices. The Portable Data Seat has additional features which provide for remote access to services as stated in section 5.2.1.15 This seat includes classified seat services);
3.
3. Remote Data Seat (SDP located outside the DARPA enclave with remote connectivity to an internal or external classified network. This seat includes classified seat services);

4. Hybrid Fixed Data Seat (Fixed Data Seat (B.1. above), which includes non-standard software or hardware);
5. Hybrid Portable Data Seat (Portable Data Seat (B.2. above), which includes non-standard software or hardware);
6. Multiple Use Data Seat (Classfied User Account which includes all Customer IT Services for users (i.e. Department of Defense (DoD) government employees, contractors, or specified liaisons) who do not require equipment for their exclusive use);
7. Windows Based Terminal (WBT) or Thin Client Seat ("terminal" device with no internal or external storage media and all classified seat services);
8. DARPA JWICS (DJWICS) Seat (SDP which includes the standard hardware and software configuration, is capable of performing local and network computing functions, and with no connectivity to the DMSS, but which is connected to JWICS. This seat includes classified seat services.); and
9. DARPA JWICS (DJWICS) Multiple Use Data Seat (JWICS User Account which includes all Customer IT Services for users (i.e. Department of Defense (DoD) government employees, contractors, or specified liaisons) who do not require equipment for their exclusive use.)

5.

C. Government-Provided Data Seats SDPs

Government-provided data seats are defined as unclassified and/or classified data furnished by the government for short-term projects that need each need user accounts, LAN drops, and access to the entire range of services described in this statement of work during a specific timeframe. An example may be IG inspection teams with their own computers temporarily assigned to DARPA for a period of time.

D. Network Services Data Seat

Network Services Seats provide all DARPA authorized computing devices (i.e. desktops, workstations, portables, servers, including SDPs with non-standard operating systems) connectivity to any servicing DARPA network and include all Customer IT services available for that network, with the exception of technology refresh. This seat does not include a Service Delivery Point.

Each data seat, with the exception of the Government-Provided Data Seat, must be available with upgrades through contractor-provided Catalog Services to augment basic functionality or support high-end, mission-essential, and/or technologically advanced functionality for certain DARPA users. User accounts for all data seats shall be provided that include access to the DARPA Enterprise Infrastructure and External Networks. Data seats shall be provided with the services described in sections 5.2, 5.3, and 5.4 of this statement of work. Each data seat supports DARPA mission-essential processes and shall include a technology refreshment rate as specified by the Service Level Agreements (SLA) included in this statement of work. Note that the contractor shall comply with current DoD regulations regarding the destruction of hard drives that contain sensitive information prior to data seats leaving the agency.

To achieve the Information Assurance goals within DoD, a Smart Card reader will be necessary with Public Key Infrastructure (PKI) enabled applications to access DoD-compliant PKI credentials. The Contractor shall provide data seats with the capability, including all required software, of supporting Smart Cards in accordance with the DoD Smart Card reader requirements in Attachment 4. The contractor may also provide DARPA users with Smart Cards in accordance with DoD specifications to be used with the Smart Card readers.

Scope: Data Seats
Reference: SLA 1,

5.1.2 Conference Room Seats

Conference room seats shall support audiovisual presentations that allow participants to conduct electronic meetings using dedicated audiovisual conferencing facilities. The services associated with these seats shall include but are not limited to: user training, Help Desk support (including VIP meeting support as requested), and integrated configuration management. The contractor shall be responsible for the maintenance (i.e. projector light bulb replacement) and repair of all contractor-owned equipment. All lighting, seating (chairs, tables, room setup), and Telco services are not the responsibility of the contractor. Conference room seats shall be comprised of the hardware, software, security features and support services provided to DARPA users as

resources. Conference room seats are defined as follows:

5.1.2.1 Portable Conference Seat

The contractor shall make available a portable digital multimedia projector with a manufacturer's rating of at least 1000 lumens, weighing less than 13 pounds, and which is capable of performing automatic synchronization, tracking, image positioning, and video source detection for use both inside and outside the DARPA enclave. A portable conference seat shall include equipment and accessories (PC/Laptop connector cable, power cable, and carrying case).
Reference: SLA 26

5.1.2.2 Basic Conference Room Seat

The contractor shall provide video presentation capability in government specified locations within the DARPA enclave. A basic conference room seat shall include equipment, infrastructure, and other services necessary to provide video presentations. The basic conference room seat includes a digital multimedia projector with a manufacturer's rating of at least 2000 lumens and which is capable of performing automatic synchronization, tracking, image positioning, and video source detection, an overhead transparency projector, projector screen and network connectivity.
Reference: SLA 26

5.1.2.3 Advanced Conference Room Seat

The contractor shall provide audiovisual presentation capability in government specified locations within the DARPA enclave. An advanced conference room seat shall include equipment, infrastructure, and other services necessary to provide audiovisual presentations. The advanced conference room seat includes a digital multimedia projector with a manufacturer's rating of at least 2000 lumens and which is capable of performing automatic synchronization, tracking, image positioning, and video source detection, a projector screen, video player/recorder capability, stereo sound systems, including dynamic speaker technology, overhead transparency projector, and network connectivity.

Reference: SLA 26

5.1.2.4 Video Conferencing Center Seats

Video conferencing center seats shall consist of high bandwidth communications that provide point-to-point and continuous transmissions that allow participants to conduct visually interactive electronic meetings between one or more distant or local sites using dedicated video conferencing facilities which include video cameras, monitors, and audio and video communications, thus enabling participants to see and hear each other as if they were in the same room. Some of the features of this capability shall include but not be limited to: room cameras with full area coverage, large monitors, on-screen menus, dynamic speaker technology, far end camera control, video player/recorder capability, software distribution and upgrades, user training, Help Desk, integrated configuration management, integration and testing, and remote diagnostics. Attachment 2 contains a description of the configuration

of current DARPA video conferencing centers. Video conferencing center seats shall be comprised of the hardware, software, security features and services provided to DARPA users as resources. Video conferencing center seats are defined as follows:

A. Unclassified Video Conferencing Center Seat

The contractor shall provide video communications at DARPA video conferencing center locations. An unclassified video conferencing center seat includes instruments, infrastructure, and other services to provide video-related connectivity within and external to DARPA. Unclassified video conferencing center seat service includes user training, Help Desk, integrated configuration management, and integration and testing. The contractor shall provide for connecting to DARPA-provided telecommunication services at each video conferencing center seat. The basic video seat price includes unlimited VTC usage between DARPA conferencing centers and other users. Basic video seat capabilities include interoperability over commercial digital services for conferencing with non-DARPA locations. The contractor shall provide operator services to include operator-assisted VTC setup and operation including off-hour support. The contractor price for unclassified video conferencing center seats shall include unlimited video conferencing sessions with other DARPA video conference centers and data seats. Calls to DARPA facilities and locations should be routed over the DARPA enterprise infrastructure. Calls to non-DARPA locations should be routed over DAPRA-provided telecommunication services.

Reference: SLA 26

B. Classified Video Conferencing Center Seat

The contractor shall provide secured (Type 1 encrypted video transmission – i.e. KIV-7 HS, KG-194) video communications at DARPA video conferencing center locations. A classified video conferencing center seat includes instruments, infrastructure, and other services to provide classified and unclassified video-related connectivity within and external to DARPA. Video conferencing center seat service includes user training, Help Desk, integrated configuration management, and integration and testing. The contractor shall provide to DARPA-provided telecommunication services and encryption devices at each video conferencing center seat. The basic video seat price includes unlimited VTC usage between DARPA conferencing centers and other users. Video seat capabilities include interoperability over commercial digital services for conferencing with non-DARPA locations. The contractor shall provide operator services to include operator-assisted VTC setup and operation including off-hour support. The contractor price for classified video conferencing center seats shall include unlimited video conferencing sessions with other DARPA video conference centers and data seats. Calls to DARPA facilities and locations shall be routed over the DARPA enterprise infrastructure. Calls to non-DARPA locations should be routed over DARPA-provided telecommunication services.

Reference: SLA 26

5.1.3 Wireless Seats

Wireless Data Seats shall include hardware, software and telecommunications services necessary to provide the ability for DARPA users to transmit and receive visual text and recorded audio sent via e-mail, phone message, or phone page from any location in the continental United States. In addition, each wireless data seat shall include internet access from anywhere in the continental United States from a portable, wireless device(s). DARPA's current wireless seat configuration is provided in Attachment 2. A

Wireless Data Seat is comprised of the hardware, software, security features and services provided to DARPA users as resources, and are defined as follows:

A. Unclassified Data
    1. Wireless Data Seat (can send and receive e-mail, and access the Internet)
    2. Wireless Data Seat Service (service only—does not include SDP)
B. Classified Data
    1. Wireless Data Seat (can send and receive e-mail, and access the Internet)
    2. Wireless Data Seat Service (service only—does not include SDP)

5.1.3.2 Wireless Voice Seats

Wireless Voice Seats shall include hardware, software and telecommunications services necessary to provide the ability for DARPA users to transmit and receive voice, text, and paging services from any location in the continental United States. International wireless voice hardware and service, where available, may be ordered in conjunction with Expert Assistance Tasks. Wireless voice seats shall also include voice mail, conference calling, call forwarding capabilities, and operator services to include directory assistance, (i.e. 411), enhanced 911 capabilities, and 24-hour operator assisted calling. DARPA's current wireless seat configuration is provided in Attachment 2. A Wireless Voice Seat is comprised of the hardware, software, security features and services provided to DARPA users as resources, and are defined as follows:

A. Unclassified Voice

    1. Standard Wireless Voice Seat (can send and receive voice and page)
    2. Wireless Voice Data Services Seat (can send and receive voice and page, and access the Internet)

B. Classified Voice

    1. Standard Wireless Voice Seat (can send and receive voice and page)
    2.

5.1.3.3 Wireless PDA Seats

Wireless PDA Seats shall include hardware, software, and telecommunications services necessary to provide the ability for DARPA users to transmit and receive electronic mail through a wireless medium. A Wireless PDA Seat is comprised of the hardware, software, security features and services provided to DARPA users as resources, and are defined as follows:

1. Blackberry Data Seat (can send and receive e-mail)

Reference: SLA: 1A, 22

5.1.4 Enterprise Infrastructure

The contractor shall provide enterprise infrastructure services that are transparent to DARPA users but are essential to DARPA network functionality, security, performance, and interoperability. "Infrastructure service" refers to the various management and operational activities, hardware, software, and transmission media necessary for the delivery of services specified in sections 5.2 and 5.3 of this statement of work to internal and external DARPA users. Enterprise Infrastructure shall include connectivity and transport services to, from, and among all DARPA Service Delivery Points (SDPs). A description of the current DARPA Enterprise Infrastructure is included in Attachment 2.

Reference: Inherent in all SLAs

5.1.5 External Networks

The contractor shall provide external network services that are transparent to DARPA users but are essential to DARPA telecommunication functionality, security, performance, and interoperability. "Network service" refers to the various management and operational activities, hardware, software, connection service, and transmission media necessary for the delivery of telecommunications services to internal and external DARPA users as specified in sections 5.2 and 5.3, and/or ordered from section 5.4 of this statement of work. External Networks shall include connectivity and transport services to, from, and among all DARPA Service Delivery Points and other non-DARPA organizations. A description of the current DARPA External Networks is included in Attachment 2. Two categories of external network services shall be provided:

A. DoD Network Service

The contractor shall provide connectivity to the National Security Agency (NSA) Intellink up to the NSA-provided interface point, and to the SIPRNET up to the SIPRNET router supplied by DISA. Intellink connectivity shall be provided for a limited number of classified data seats. SIPRNET connectivity shall be provided for any and/or all classified data seats, classified video conferencing center seats, and classified wireless seats. Connectivity to Intellink and the SIPRNET shall be provided with sufficient bandwidth to meet performance specifications, service levels, and security requirements as stated in Attachment 3. DARPA's existing DoD Network services are pictured in Attachment 2. Additional connections necessary to meet mission-essential requirements may be ordered under the contractor provided catalog services.

Reference: SLA 27, 27A

B. Commercial Network Service

The contractor shall provide connectivity to commercial network services including to the internet from each data, video conferencing center, and wireless data seat type with sufficient bandwidth to meet performance specifications, service levels, and security requirements as stated in Attachment 3. DARPA currently obtains internet access from commercial service providers through agreements between the service providers and the incumbent contractor. DARPA's existing network services are pictured in Attachment 2.

Reference: SLA 27

5.1.6 Printer Seats

A printer seat is a service delivery point comprised of the hardware, software, security features and services necessary for DARPA users to perform either local or network printing functions and to receive information technology services as defined in section 5.2 and Service Level Agreements. Printer seats must be compatible with all data seat service delivery points provided by the Contractor. Printer Seat Service Delivery Points shall be proposed by the Contractor and reviewed and approved by the Configuration Control Board (CCB) as described in section 5.2 of the Statement of Work.

The printer seats are defined as follows:

A. Personal Printer Seats
    1. Contractor shall have the option to install locally or make available on the network.
    2. Color Printer (must have a manufacturer's rating of at least 6.5 ppm black and white, 5 ppm color, 5,000 pages per month, 600 dpi black and white, 1200 dpi color, and have a paper-tray capacity of no less than 150 sheets.)
    3. Black and White Printer (must have a manufacturer's rating of at least 15 ppm, 10,000 pages per month, 1200 dpi and a paper tray capacity of no less then 250 sheets.)

B. Departmental Printer Seats
    1. Includes functionality to allow it to be available on the network and available to users.
    2. Color Printer (must have a manufacturer's rating at least 16 color ppm, 65,000 pages per month, 600 dpi, have a paper-tray capacity of no less then 700 sheets, and duplex printing.)
    3. Black and White Printer (must have a manufacturer's rating of 25 ppm, 150,000 pages per month, 1200 dpi, have a paper-tray capacity of no less then 1000 sheets, and duplex printing.)

C. Enterprise Printer Seats
    1. Includes functionality to allow it to be available on the network and available to users.
    2. Color Printer (must have a manufacturer's rating at least 16 color ppm, 65,000 pages per month, 1200 dpi, have a paper-tray capacity of no less then 700 sheets, and provide for duplex printing.)
    3. Black and White Printer (must have a manufacturer's rating of 32 ppm, 150,000 pages per month, 1200 dpi, have a paper-tray capacity of no less then 1000 sheets, and provide for duplex printing.)

Printer seats shall be provided with the services described in sections 5.2, 5.3, and 5.4 of this statement of work. Each printer seat supports DARPA mission-essential processes and shall include a technology refreshment rate as specified by the Service Level Agreements (SLA) included in this statement of work. Printer seats already deployed in the DARPA enclave shall be exempt from manufacturer's ratings requirements, but must be refreshed as specified by the Service Level Agreements (SLA) included in this statement of work.

Reference: SLA 9, 36C

5.1.7 Introduction of Potential Service Delivery Points (PSDPs)

A DARPA customer can initiate the introduction of a PSDP by requesting it via the contractor-supplied catalog. If the government determines there is a requirement for the requested PSDP, the contractor shall initiate the Configuration Control Board (CCB) and shall create an Expert Assistance Task (EA) for the procurement of the PSDP and interoperability and integration testing. If the PSDP is approved by the CCB, the contractor shall add it to the COTS Catalog. The government will then place a COTS catalog order on behalf of the requesting DARPA customer, and the contractor shall deliver the PSDP to the customer. If the customer cancels the order, the PSDP is not classified as a SDP (See Section 5.1), or the SPDP cannot be returned to the original vendor, it will be retained as an in-stock item; its disposition will be reflected on the Credit/Asset report, and it will be available to the Government until fully depreciated.

The government may require the contractor to propose a CLIN for the PSDP. If the government approves the CLIN, the contract will be modified to include the new seat CLIN and seat order. In the event no CLIN is created for the PSDP, the contractor shall make the PSPD available for ordering from the COTS catalog.

This process is illustrated in attachment 8: DARPA COTS Seat Process Flow Diagram.

5.2 Customer Information Technology (IT) Services

DARPA Customer IT Service Elements are arranged in seven Service Categories. These categories include Basic User Services, Help Desk Services, Communications Services, Systems Services, Information Assurance Services, Logistics Services, and Program Management Services. These services are necessary to provide basic functionality and shall be included in all Service Delivery Points as basic services.

Each of the seven Service Categories is described below along with their constituent Service Elements. For each, there is a brief description of the service. The description is followed by identification of the scope of the service (Scope) and a list of notional service level agreements (SLA) contained in Attachment 3 that may be used by the Government in evaluating contractor performance in delivery of these services to the DARPA customer.

5.2.1 Basic User Services

The contractor shall provide the following services to each DARPA user. The current DARPA standard and non-standard but DARPA-supported hardware and software is defined by the Configuration Control Board (CCB) .

5.2.1.1 Standard Office Automation Software

Requirement: The standard data seat integrated software suite shall include word processing, spreadsheet, presentation graphics, database, calendaring, a collaborative work environment, forms processing, browser, and virus protection tools. The data seat shall provide the capability to view, hear, manipulate and manage information consisting of text, graphics, images, video, and audio. This shall also include processing and rendering of the multimedia data being transferred from any source. COTS software to

support advanced and/or specialized functions beyond those provided as standard office automation tools shall be available and may be purchased separately from contractor catalog services.

Scope: Basic service requirement for all Data and Video Conferencing Center seats.
Reference: SLA 2

5.2.1.2 E-mail Services

Requirement: The contractor shall provide services for sending, storing, processing, and receiving e-mail and multimedia e-mail attachments. The services shall be configurable to provide Medium Grade Service (MGS) capability for sending and receiving signed and encrypted e-mail and attachments, by utilizing DoD Public Key Infrastructure (PKI) compatible user certificates, and interoperable with MGS systems outside the DARPA domain. MGS shall be provided with e-mail packages that support cryptographic functions from a smart card. Each seat should be supplied with e-mail capability and file transfer management tools. E-mail is an integral part of DARPA, and shall conform to industry standards (e.g., native RPC, HTTP, IMAP4) for interoperability and remote access and comply with DARPA conventions for domain naming (i.e. retention of DARPA.mil domains). The contractor will ensure that foreign nationals are clearly identifiable in electronic communications in accordance with DoD Directive 5230.20.

Scope: Data and Video Conferencing Center seats.
Reference: SLA 3

5.2.1.3 Directory Services (DS)

Requirement: The contractor shall provide and maintain global information services delivering a distributed computing environment that supports the management and utilization of file services, network resources, security services, messaging, web, e-business, white pages, and object-based services across DARPA. Information services shall include storing, updating, and publishing directory information from multiple systems and formats including e-mail addresses, commercial and DSN telephone numbers, certificates, addresses, applications, network devices, documentation and routing information, as well as other data and/or resource in support of the DARPA IT environment. The contractor shall ensure directory entries conform to Government standards and provide the flexibility to include users not directly supported by the contractor in Directory Services (DS). DS shall support the ability for end users to interact globally (anywhere, anytime) with the network directory services in a transparent and consistent manner.
The DS should support and facilitate the following basic functions:

1. Supported by PKI authentication services, provide the capability for users, devices, and applications to discover and utilize global information services data.

2. Support the monitoring of administration and management of network resources.

3. Support the implementation of global account management and subsequent authentication and authorization to data maintained in the global directory service.

4. Support the enablement and distribution of applications.

5. Provide a proactive environment that builds and manages relationships between objects within the global directory service.

Scope: Basic service with all data, video conferencing center, and wireless data seats.
Reference: SLA 4

5.2.1.4 Fax Services

Requirement: The contractor shall provide the capability and features that allow users to send outgoing faxes and receive incoming faxes via routing through email. For outgoing faxes, the contractor shall provide for automatic generation of a user-defined outgoing fax cover sheet from DARPA users from any data seat type, and the transmission of a fax based on selection of an electronic file as an attachment to the fax cover sheet. Incoming faxes shall be routed to the DARPA user recipient via email.

Scope: Basic service with all data, video conferencing center, and wireless seats.
Reference: SLA 8

5.2.1.5 Internet Access and Services

Requirement: The contractor shall provide the capability and features that allow users to access in-house and external web content. The contractor shall provide communication with web host servers on the DARPA network and on the Internet.

Scope: Basic service with all data, video conference center, and wireless data seats.
Reference: SLA 6, 12

5.2.1.6 News Group Services

Requirement: The contractor shall provide services for posting, reading, and processing user-determined public and private newsgroups. The contractor shall also provide news feed services as may be identified and obtained from Catalog Services.

Scope: Basic service with all data, video conference, and wireless data seats.
Reference: SLA 7

5.2.1.7 Print Services

Requirement: The Contractor shall provide to end users the capability and features to produce black and white and color hard copies of electronic documents. The contractor shall provide connectivity to government-furnished printing and duplicating machines located on each floor of DARPA to enable high-speed and quantity printing services. The DARPA current standard duplicating machine is a Xerox Docutech Document Center Model 4605T.

Scope: Basic service with all video service center seats and data seats when attached to the DARPA enterprise infrastructure.
Reference: SLA 9

5.2.1.8 DARPA Intranet

Requirement: The contractor shall provide and maintain a DARPA intranet that provides a point of entry for data, and wireless seats into the DARPA enterprise infrastructure. The contractor shall provide a service whereby DARPA users may access data and files from remote locations, and search the contents of DARPA intranet web pages. The contractor shall provide the capability for web-crawling, site indexing, and an efficient search engine. The service shall exclude authoring of the web content and application development, which may be ordered under the contractor catalog services. The contractor shall provide web/Intranet support to DARPA organizations which have created intranet content that extends beyond the scope of DARPA Intranet Services. This support will be limited to tasks and activities associated with junior to mid-level support and will consist of tasks that do not require senior developer expertise or engineering support. Examples of these tasks include, but may not be limited to the following:

- Code Reviews
- Tool usage support and direction
- Troubleshooting and instruction
- Basic site management

The contractor shall identify and define the level of effort required for any support requests that necessitate engineering/senior development services that extend beyond the scope of the web/intranet support For users located outside a DARPA firewall, the contractor shall provide the capability to access the DARPA Intranet with security features. Virtual Private Network (VPN) solutions may be used, but VPN devices used within DARPA shall be selected and implemented in consultation with DARPA security personnel. Information regarding DARPA's current VPN service is provided in Attachment 2.

Scope: Basic service for all data and wireless data seats.
Reference: SLA 6

5.2.1.9 Classified Network Connectivity

Requirement: The contractor shall provide the means for classified data seat access to SIPRNET and Intellink, and JWICS.

Scope: Basic service with all classified data seats.
Reference: SLA 11, 27A

5.2.1.10 Desktop Access to Government Applications

Requirement: All Government-off-the-shelf (GOTS) legacy systems and applications in operation at the time of order shall continue to function as at the time of order. These systems and applications include desktop-loaded and server-hosted applications for financial and personnel functions. COTS software beyond that provided by the vendor as standard office automation may be purchased separately under contractor COTS catalog. To provide solutions to fulfill emerging requirements for software re-engineering, transition of legacy applications or development of new applications, technical services may be ordered under the contractor provided Expert Assistance Catalog. Applications and functionality obtained from the contractor Expert Assistance Catalog must be integrated into and function seamlessly

within the DARPA information technology environment.

Scope: Basic service with all data, video conferencing center, and wireless data seats.
Reference: SLA 14

5.2.1.11 Moves, Adds, Changes, and Deletes (MACDs)

Requirement: For User Requested MACDs, the contractor shall provide services to perform user-requested system hardware and software changes of data, video conferencing center, printer, and/or wireless seats. This applies where service within this statement of work exists.

MACDs include the following:

- De-installation, move, re-installation, or change of data, video conferencing center, or wireless seat hardware.
- Creation, modification or deletion of a user account including email and directory services.
- A change in service delivery point type.
- A contractor periodic or unscheduled software refresh or update.

Scope: Basic Service with all data, video conference center, printer and wireless data seats. For planning purposes, three user-requested MACDs per year are anticipated for each ordered data, and wireless seat. User requested moves of video conferencing center seats are not anticipated but two MACDs should be anticipated.
Reference: SLA: 15

5.2.1.12 Software Distribution and Upgrades

Requirement: The contractor shall provide the capability to distribute new and upgraded software with the method of installation and distribution resulting in transparency of functionality from the end-user perspective in accordance with best business practices and the schedule specified in the SLAs identified below. This capability includes COTS software, GOTS software, custom applications software developed by other parties and integrated by the contractor, and deliverables ordered from contractor catalog services.

Scope: Basic service with all data, video conference center, printer, wireless data seats enterprise. infrastructure and external networks.Reference: SLA 2, 16

5.2.1.13 User Training

Requirement: For each change in services and/or applications, the contractor shall analyze, identify, and implement the form of training most effective and efficient for DARPA users. Space for classroom-based user training will be provided by DARPA in government or contractor-occupied facilities. Hardware, software, equipment, training materials, and supplies necessary for effective training shall be provided by the contractor. Automated user training solutions used by the contractor shall incorporate advanced distance learning solutions. User training shall be made available as a result of the following for all data, video conference center, and wireless seats including, as a minimum:

Initial Implementation

Implementation of a change in technology or user interface

Identification of user knowledge shortfall (e.g. as a result of a Help Desk call or user-invoked systems failure)

Move/Add/Change

Annual security training requirement for users

Upon contracting officer representative (COR) request

Scope: Basic service for all data, video conference center, and wireless seats.
Reference: SLA 17

5.2.1.14 Public Key Infrastructure (PKI) Integration

Requirement: The contractor shall provide for the establishment, integration and management of the DARPA Public Key Infrastructure (PKI) Service in compliance with DoD PKI security policies and guidelines. The DARPA PKI Service shall include directory support, registration (operation of Local Registration Authority (LRA)), interface to related DARPA systems, hosting of PKI-enabled servers, and required key management services as well as PKI solutions for email, web applications, file transfer, and Virtual Private Networks. The Government will provide the contractor with the DoD PKI user profiles as GFI to be implemented by the contractor within DARPA. Certification Authority (CA) functions will be performed by the government. LRA functions shall be performed by the contractor.

Scope: Basic service for all seats and enterprise infrastructure and external network service delivery points.

5.2.1.15 Remote Access Service

Requirement: The contractor shall provide services that allow users to access the DARPA intranet and data network from remote locations via a local or toll-free call 24 hours per day, 7 days per week. The service shall provide for the identification and authentication of the user via DoD PKI Certificates on the DoD Common Access Card or equivalent smart card provided by the contractor. The service shall authorize access to a DARPA-defined set of services, with capacity available to accommodate DARPA surge requirements.

Scope: Basic service for all portable, remote, hybrid and wireless data seats.
Reference: SLA 18, 19

5.2.1.16 Web Services

Requirement: The contractor shall provide web hosting as a service for DARPA web sites, including storage and processing of web content. This service includes DARPA internal access, public access, and classified hosting. Identification and Authentication (I&A) and Access Control to DARPA as well as to DARPA and DoD secure websites will occur via DoD PKI compatible certificates stored on either the

DoD Common Access Card (CAC) or equivalent smart card provided by the contractor. As part of this service, the Contractor shall provide statistics regarding web access. The service does not include authoring of web content and application development, although those services may be ordered under the contractor provided Expert Assistance Catalog.

Scope: Basic service for enterprise infrastructure.
Reference: SLA 6

5.2.1.17 Shared File Services

Requirement: The contractor shall provide the ability for users to store and retrieve files on shared, controlled access storage media. This includes access controls, and back up and recovery. DARPA currently imposes no quotas for users on file storage or e-mail storage. Recognizing the need to do so, the contractor shall provide recommendations to DARPA based on industry best practices, regarding the maximum practical amount of disk space that should be assigned to each service delivery point type given DARPA's mission requirements. Such recommendations shall be included as part of SLA reporting.

Scope: Basic service for all data, video conference center, and wireless data seats.
Reference: SLA 5

5.2.1.18 Retention of DARPA Electronic Records

Requirement: The contractor shall provide for retention of electronic information files consistent with applicable DoD Standard 5015.2-STD and the National Industrial Security Program Operating Manual (NISPOM).

Scope: Basic service for all data seats.
Reference: SLA 13

5.2.1.19 Disaster Recovery Services

Requirement: The contractor shall provide for disaster recovery planning, offsite secure storage of data and files, and training for DARPA personnel in the event of a disaster. In addition, the contractor shall make provisions for restoration of services in a different location within 24 hours in the event of a disaster. The contractor shall implement industry best practices, DoD policy and the provisions of the National Industrial Security Program Operating Manual (NISPOM).

Scope: Basic service for all data, video, and wireless seats.
Reference: SLA 29

5.2.2 Help Desk Services

Requirement: The contractor shall provide world-class user technical assistance via desk-side service, phone, e-mail, or fax for solving information technology service-related issues to the user's complete satisfaction. This includes providing an integrated service with a single point of contact for all DARPA users. DARPA users shall have the capability to interact or communicate with the Help Desk by voice, email, fax, web and/or by personal visit to an onsite help desk located in DARPA-provided office space. In addition, Help Desk Services shall include junior and mid-level support for service requests that extend

beyond the basic user services and problem resolution associated with Help Desk support. These service requests will be supported and documented within the automated support request system. Examples of these types of service requests include, but are not limited to, the following:

- Virus scanning of disks
- Burning of CDs
- Data copies/moves/conversion/organization/migration
- SW/HW installation and re-configuration

The contractor shall identify and define the level of effort required for any service requests that necessitate engineering services that extend beyond the Helpdesk support and service request spectrum. The contractor shall provide escalation services with procedures to be reviewed and approved by DARPA and implemented by the contractor. These services shall include the timely notification of DARPA personnel by the Help Desk of planned or unplanned system maintenance or degradation of DARPA's information technology services.
Additionally, designated DARPA users shall have visibility into a web-based trouble ticket status system. Because Help Desk service is mission-essential for the DARPA user community, the contractor must provide a high caliber of service and support. The provisions of FAR 52.237-3 (c) applies to the incumbent contractor.

Scope: Basic service for all users.
Reference: SLA 23

5.2.3 Communications Services

Requirement: The contractor shall provide systems services with security features in accordance with the requirements in the following subparagraphs.

5.2.3.1 Metropolitan Area Network (MAN) and Wide Area Network (WAN) Connectivity

Requirement: The contractor shall provide metropolitan area network (MAN) and wide area network (WAN) connectivity between geographically separated DARPA users and devices. Such service shall provide connection to current DARPA locations identified in contractor submitted reports to meet the requirements of Section 5.2.4.5 as well as the current level of connection to the Internet. Additional network connection services needed in the future may be ordered from contractor provided catalog services. The Network Diagram in contractor submitted reports identifies the interface requirements applicable to existing DARPA MAN and WAN connectivity. The contractor may be able to transfer agreements the incumbent contractor holds with existing MAN and WAN providers. The provisions of FAR 52.237-3 apply to the contractor.

Scope: Basic service for Enterprise infrastructure and external networks.
Reference: SLA 24

5.2.3.2 Local Area Network (LAN) Communication Services

Requirement: The contractor shall provide the capability to interconnect geographically co-located and separate DARPA Local Area Networks (LANs) and attached devices. The current LAN configuration is

provided in Attachment 2.

Scope: Basic service for Enterprise infrastructure and external networks.
Reference: SLA 25

5.2.4 Systems Services

Requirement: The contractor shall provide systems services with security features in accordance with the requirements in the following subparagraphs.

5.2.4.1 Network Management System (NMS) Service

Requirement: The contractor shall provide services that include fault management, configuration management/asset management, account management (for empirical user data and fiscal accountability), performance management, and security management. These services shall be provided in accordance with the Service Level Agreements in Attachment 3. The contractor shall make available to designated Government entities, near real time information feeds to support Government oversight, maintain accessible historical data, provide summary management reports that detail the NMS functions, and allow DARPA and the contractor to forecast its future networking requirements through the use of modeling techniques.

Scope: Basic service for all Enterprise infrastructure and external networks.
Reference: SLA 28

5.2.4.2 Operational Support Services (OSS)

Requirement: The contractor shall provide services that include, but are not limited to, data backups and recovery, data archiving, routine database audits and maintenance, log retrieval and audits, purging of records, and network address administration. The contractor shall support Government oversight, maintain accessible historical data, and provide summary management information that details the OSS functions. Network operations displays shall be provided to users authorized by DARPA on a real-time basis, indicating status of network assets. The display shall be available to authorized users at any data seat connected to the DARPA network and show performance status of the overall network and individual servers and routers.

Scope: Basic service for DARPA Enterprise infrastructure.
Reference: SLA 29

5.2.4.3 Technology Refreshment, Insertion, Enhancement and Capacity Planning

Requirement: The contractor shall provide capabilities to support the technological evolution and planning of changes to the DARPA infrastructure, specifically to estimate future requirements, capabilities, volume, usage, and application characteristics, as well as integration of emerging technology to meet the evolving requirements of DARPA. These capabilities shall be provided for all service delivery points, and include periodic analysis of enterprise infrastructure and external network capacities along with recommendations for future engineering changes for Government review and approval.

For Hybrid Data Seats, external hardware peripherals and software products acquired through the COTS

Catalog and compatible with the refreshed data seat will be migrated to the refreshed Hybrid Data Seat. If any internal components, external hardware and/or software products are determined to be incompatible or not standard (i.e. a larger harddrive) within the refreshed data seat, the Contractor shall offer the DARPA end-user alternative solutions which provide similar or better functionality through the COTS catalog and/or the Expert Assistance service.

Scope: Basic service for all service delivery points.
Reference: SLA 30, 36C, 36D

5.2.4.4 Domain Name Server (DNS)

Requirement: The contractor shall provide Domain Name Server (DNS) services that include the address resolution of Uniform Resource Locator (URL) to IP addresses. This capability shall include both internal DARPA URLs as well as external URLs. The services shall meet all functionality of the current Domain Name Server (DNS) service, to include flexible support for offsite locations to retain the darpa.mil domain name convention. The contractor shall manage the DARPA network addresses.

Scope: Basic service for enterprise infrastructure.
Reference: SLA 31

5.2.4.5 Data Reporting

Requirement: The Contractor shall electronically post the following information for on-line and/or secure internet access by designated DARPA personnel. Reports shall be in contractor format. The contractor is encouraged to post data in a database format, with access via selectable report formats. At a minimum, the following data shall be provided:

Type	Title	Contents	Frequency
Service Levels	SLA Data Report	Data showing service levels provided for period	Monthly
	Order Status Report	Data shall include ordering office, order number, order date, order status, back order date, ordered amount due, date order created, order created by I.D., date order last modified, number of ordered products, ordered product, product number, quantity, order product status and unfilled orders status, quantity shipped, date shipped, quantity installed, and order price.	Monthly
	Asset and Credit Report and Asset Management Database	Data shall include description of asset, location of asset, quantity of asset, assessment line item number, date of assessment, plant property value, age, life cycle duration and cost, proposed/actual credit amount, delivery order number, deductive delivery order amount, line of accounting, funding document number, funding document description, delivery order description, commitment amount, obligation amount, and expenditure amount.	Monthly (maintained continuously)
	Incentive Report	Data shall include order or modification number, date and amount, description of incentive, date of audit, and date of incentive payment.	Monthly
Security	Incident Report	Data shall include any configuration changes, computer incidents, network incidents, INFOCON status, and intrusion detection reaction alert status.	Within 24 hours of incident
	C&A Documentation	Data shall include the following: • System Security Authorization Agreement (SSAA) • Risk Assessments • Vulnerability Assessments • Risk Mitigation Plans	SSAA: Initial draft 30 days after placement of first order, second delivery 90 days after placement of first order, third delivery 180 days placement of first order, with revisions if

			there are any significant architecture changes at any other time. All other requirements due annually, at a minimum.
	Security CONOPS (Including Disaster Recovery Plan)	Data shall include a security concept of operations and a disaster recovery plan in accordance with industry best practices and DoD regulations.	Within 45 days of placement of first order and updates semi-annually thereafter.
	Security Critical Product Selection	Data shall include a listing of all IA mechanisms, to include but not be limited to the following: firewalls, intrusion detection systems, virtual private networks, security management tools, operating system for server and user workstations, smart card reader, etc.	15 days after placement of first order and within 10 working days of changes
	Security Status Report	Real time or near real time data feed supporting government oversight of security functions.	Continuous commencing at the end of transition to full performance
	Security Procedures	Data shall include security procedures describing how IA mechanisms will be operated to provide the security services specified in the statement of work.	Delivery with initial seats, updates with changes
	GFE Type 1 Crypto Requirements	Data shall include a detailed listing of required GFE Type 1 crypto devices. Data shall include the following at a minimum: quantity of Type 1 crypto required, classified key material required, dates required for both crypto and classified key material.	Within 15 days of placement of first order, updates with changes
Architecture	Configuration Management/Diagram Reports	The documentation will provide a systems architecture view of the DARPA network in the contractor's standard format. The documentation will include a full description of all external interface points, to include DoD compliant technologies, protocols, and peering arrangements for external connectivity. It will include physical and logical connectivity, and how interoperability is achieved at the interfaces. The architecture will detail DARPA network hosting of legacy systems. Data shall include graphic architecture designs and cabling diagrams, at least to the building level.	15 days after placement of first order, and within 5 working days of changes
	Network Connectivity Plan	Data shall include network topology showing WAN/LAN connectivity. All external interface connection points (SIPRNET, Intellink, Internet, etc.) shall be clearly annotated.	15 days after placement of first order and within 10 working days of architecture changes
	Security Architecture	Data shall include architecture diagrams that depict how information is transferred through defense in depth boundaries 1 through 4 (e.g., from WAN connections at boundary 1 to interior destinations, down to hosts on LAN at boundary 4). Diagrams should include the proposed employment of all major network components (at a minimum in-line network encryptors, firewalls, intrusion detection systems, servers, routers, switches, load-balancers, and data path) which play a significant role in network operation, management, and security. Diagrams shall also indicate location of alternate paths and backup equipment. This includes information sources, supporting paths and capacities, any unique manipulation of data in transit, points of termination and placement of all proposed security components. The diagrams shall be in contractor format. Diagrams shall address both unclassified and classified architectures, and also any unique architectural differences associated with different types of locations.	15 days after placement of first order, and within 10 working days of architecture changes.
Transition	Fielding and Transition	The contractor shall generate a transition plan, which will provide the means	Within 30 days

Planning	Plan	for coordinating system, product, and service rollouts and tests with the Government. This plan shall reflect the actions identified in the Risk Assessment, C&A, and Security CONOPS (including Disaster Recovery Plan) (as shown above), and Interoperability Test Plan.	of placement of first order.
Video	Configuration Management Report	Provide data sufficient to identify configuration management of service delivery points.	Within 30 days after contract award. To be updated on a monthly basis.
Network Management System Service	Information Feeds for Government Oversight	Historical data summary and management reports detailing NMS functions in contractor format.	Continuous commencing at the end of transition to full performance
Integrated Configuration Management	Logical Relationship Record	Logical relationship record of items and asset inventory.	24 hours after change
Program Management	Program Management Plan	The contractor shall generate and maintain a program management plan, which will provide the means for managing and administering the services provided in this statement of work. This plan shall include standard operating procedures, processes and methods as they apply to performance of the entire statement of work. This plan shall also include the contractor's initial assessment of the requirements in section 5.3.6 of the statement of work, and address how the contractor will ensure ongoing compliance with this requirement.	Within 5 days after contract award. To be updated within 30 days and quarterly or more often if needed thereafter.
Transition	Initial Contract Transition Plan	The contractor shall generate and maintain an initial contract transition plan, which will provide the means for managing and administering the orderly transition of services from the incumbent contractor.	Within 5 days after contract award.
	End of Contract Transition Plan	The contractor shall generate and maintain an end of contract transition plan, which will provide the means for managing and administering the orderly transition of services to a follow-on contractor or any party designated by the Government.	Within 30 days of request

5.2.5 Information Assurance Services

Requirement: The contractor shall provide Information Assurance services with security features in accordance with the requirements in the following subparagraphs.

5.2.5.1 DARPA Security Operational Services

Requirement: The contractor shall provide security services for protection of the Information Systems, Information System Domains (Communities of Interest), and Information Content (at rest, in use, and in-transit) in accordance with DoD Information Assurance policies and procedures. These security services shall be provided to protect both non-classified and classified information. These operational security services shall be fully integrated with DARPA PKI services to ensure confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall implement the necessary Information Assurance (IA) mechanisms to provide these security services, and shall conduct vulnerability assessments to validate that the necessary controls are in place to satisfy the IA requirements for DARPA. As part of implementing these security services, the contractor shall be responsible for implementing Government directed IA mandates such as INFOCONs (information operations conditions) and IAVAs (information assurance vulnerability alerts). Implementation of IA mandates shall be accomplished within Government specified timeframes. The contractor shall also be responsible for ensuring that the DARPA infrastructure meets the requirements for certification and accreditation in accordance with DoD policy and SLAs. As part of these security services, the contractor shall make available near-real time data feeds, or provide real-time data feeds where available, to support

Government oversight detailing the security operational functions.

Scope: Basic for all DARPA Service Delivery Points and Services.
Reference: SLA 33

5.2.5.2 DARPA Security Planning Services

Requirement: These strategic security services shall provide for DARPA to enhance the confidentiality, integrity, availability, authenticity, and non-repudiation requirements. The contractor shall support the use of mechanisms including, but not limited to, encryption, access control, user identification and authentication, malicious content detection, audit, and physical and environmental control. The contractor shall make available in accordance with the SLA, periodic information feeds to support Government oversight, maintain accessible historical data, and provide summary management reports that detail the security planning functions. The contractor shall conduct vulnerability assessments in accordance with DARPA direction and DoD policy. On a quarterly basis, the contractor shall propose updated and/or revised architecture and/or configuration change designs to accommodate changing requirements, emerging technology, and results of vulnerability assessments, for Government review and approval.

Scope: Basic for all DARPA Service Delivery Points and Services.
Reference: SLA 36

5.2.6 Logistics Services

Requirement: The contractor shall provide logistics services with security features in accordance with the requirements in the following subparagraphs.

5.2.6.1 Integrated Configuration Management (CM)

Requirement: The contractor shall develop and implement an effective configuration management control process whereby DARPA personnel and their designees shall participate in a contractor-managed configuration control board that reviews all technology refreshment, technology insertion, or technology enhancement changes proposed by the contractor for each section of this statement of work on a quarterly basis. The board shall examine the benefits to be achieved for DARPA in terms of effectiveness and efficiency, and assess the impact of proposed technology refreshments on contract cost. DARPA designated personnel must authorize all technology refreshment changes proposed for addition to any section of the statement of working the event the proposed change departs from the current architecture and/or product suite used within DARPA. All configuration changes that require adjustments in contract price must be approved by the Contracting Officer. The contractor shall maintain a Configuration Management System including an asset inventory of all hardware and software. In addition, the contractor shall maintain a logical relationship record of the items in the asset inventory. Changes to the assets inventory shall be reflected in the configuration management system no later than 4 hours after the change. The logical relationship record shall reflect updates no more than one hour after the change.

Scope: Basic service for all service delivery points and services.
Reference: SLA 36A

5.2.6.2 Integration and Testing

Requirement: When the contractor modifies the user's existing configuration, (e. g., during initial seat fielding, applying maintenance or technology refreshment, insertion or enhancements), the contractor shall:

(a) Minimize the time involved to complete the configuration modification to achieve the updated baseline.

(b) Test prior to deployment, and coordinate system, product, and service roll outs with the government to facilitate implementation and to minimize impact to users. Coordination with the government shall include agreement on the scope of interoperability testing and assessment of impact to DARPA users.

(c) Maintain interoperability among the various seat configurations. A modification to any existing baseline configuration, which was interoperable prior to the modification, shall maintain at least the same level of interoperability after the modification is fully integrated.

(d) Maintain interoperability with extranets and relevant non-DARPA provided components of the DOD Global Information Grid. Interoperability shall not be affected by any modification of the user's existing configuration.

Scope: Basic service for all service delivery points.
Reference: SLA 36B

5.2.6.3 Transition Planning

Requirement: Transition planning support for DARPA organizations shall include migration of the current "as-is" information technology service to the desired “to be” level of service, both for initial deployment of new capabilities ordered from Catalog Services and during ongoing technology refreshment, insertion and enhancement of service delivery points under this contract.

Scope: Basic service for all service delivery points.
References: SLA 36C, 36D

5.2.6.4 Interoperability Test Plan

Requirement: The contractor shall develop an interoperability test plan and procedures that will minimize the possibility of interoperability problems during modification of user existing configurations. The contractor shall verify that interoperability is intact upon completion of the modifications, and provide for interoperability monitoring during service provisioning.

The Interoperability Test plan shall also provide for a series of mechanisms that detect unacceptable trends in performance that indicate that the software and hardware installed, component settings, and/or procedures are not in compliance, and must be corrected to support interoperability. This test plan shall address interoperability and availability as it relates to the delivery of functionality associated with service delivery points, customer IT services, IA/CND services, items ordered from catalog services, and work performed as part of transition services.

The test plan reporting criteria shall include a threshold level, agreed to by Government and the contractor, that requires immediate notification of the Government and appropriate action by the contractor to correct. Corresponding SLAs are prescribed for these services and they stipulate response times to Government for exceeding these threshold levels and correcting related deficiencies. The test plan will be proposed by the offeror and approved by the Government for implementation in accordance with the appropriate SLAs.

As part of initial contract transition planning, the government will provide an Operational Architecture (OA) for the specific segment being transitioned, installed, integrated or modified. This Initial Operational Architecture will illustrate DARPA information flows among selected organizations. The contractor shall ensure that interoperability among and between DARPA and all existing non-DARPA components, including those defined in the OA, is maintained during the modification. The contractor's Interoperability Test Plan shall verify interoperability after segment installation and integration completion. As part of post modification testing, interoperability testing shall include, but is not limited to, a verification of the interoperability of the applications from the list provided at as part of the initial OA that are legacy to the segment being modified. The initial government OA will define the applications that are legacy to the segment being installed and integrated or modified. The initial government OA does not alleviate the contractor of the contract requirement to maintain the interoperability of legacy applications.

References: SLA 36B

5.2.6.5 Critical Applications

The contractor shall provide data seat interface and enterprise infrastructure service for critical legacy applications developed and maintained by others that will be provided as GFI to the contractor. The contractor shall provide desktop access, infrastructure and other services necessary to house the applications with basic service functionality on the DARPA network. The contractor shall coordinate with legacy applications owners to ensure the smooth and uninterrupted operation of legacy applications. Such legacy applications include the DARPA financial management system, suspense tracking system, personnel system, and DBWebGenerator, a web page generation tool provided to DARPA users. Attachment 5 (Y2K Plan) contains a list of all DARPA legacy applications

Scope: Basic service for all data seats, enterprise infrastructure and external networks.
Reference: SLA 14

5.2.7 Program Management Services

The contractor shall provide program management services for the entire statement of work in accordance with the requirements in the following paragraphs.

5.2.7.1 Management and Administration

Requirement: The contractor shall provide effective, efficient and responsive program and project management, financial management, and contract administration services for this entire statement of work. The contractor shall report the status and progress of each item of work being performed on a monthly basis and shall submit a monthly Financial Report. The contractor shall hold in-process reviews

on a quarterly basis with DARPA personnel. Items for discussion include strategic planning, contractor and government performance with respect to quality, schedule, and cost, summary review of detailed Plan of Action and Milestones (POA&M) for each initiative, metrics that portray the progress of work under the contract, a summary of the quality of work performed from the points of view of DARPA customers, and recommendations for improvement of both the contractor and government staff to achieve more effective and efficient support of the DARPA mission.

Requirement: The contractor shall develop and maintain a project management methodology for planning, control, and risk management including communicating and executing individual task requirements and resolving technical, service, and management issues and risks. The methodology shall include, but not be limited to: 1) strategic vision to include technology and service delivery; 2) advocating the service delivery concept within DARPA; 3) resolving short notice mission critical requirements or problems; 4) contractor organization and account management (who will be responsible for DARPA accounts and their specific roles); and 5) identifying, executing, and reporting key milestones and events (both one-time and recurring that may extend beyond service level metrics). The contractor shall also develop and maintain a Project Management Plan (PMP) that identifies the operational and organizational relationship that will exist between contractor and DARPA personnel. Within two weeks of contract award, key personnel shall be identified as agreed by DARPA and by the contractor.

Scope: Entire SOW.
Reference: SLA 39

5.2.7.2 Outreach

Requirement: The contractor shall perform proactive communications and outreach with DARPA users to inform them about services provided in this statement of work. The contractor shall provide current collateral such as brochures, briefings, seminars, white papers, flyers, web content, etc. targeted to DARPA users. The contractor shall conduct information sessions and facilitate focus groups of DARPA users on a monthly basis to provide information and receive user feedback about the information technology services provided under this statement of work. The contractor shall form a supportive and close working relationship with other DARPA contractors performing work impacted by or related to this statement of work.

Scope: Basic service for all service delivery points.
Reference: SLA 40

5.3 Information Assurance/Computer Network Defense (IA/CND) Services

Requirement: The contractor shall implement the information assurance/computer network defense requirements outlined in the following paragraphs

Scope: Basic service for all service delivery points.
Reference: SLA 27A, 33, 34, 36

5.3.1 General DoD and DARPA IA Policies

Requirement: As specified in DoDD 5200.28 (Security Requirements for Automated Information Systems (AISs), DoDI 5200.40 (DoD Information Technology Security Certification and Accreditation

Process - DITSCAP), DoD 5200.2-R (DoD Personnel Security Program), all automated systems and services shall meet fundamental security requirements and must be accredited by the Designated Approving Authority (DAA) prior to processing classified or sensitive non-classified data. The provision of all IT services in this entire statement of work shall be implemented with proper products, policies, and procedures to ensure required system certification and accreditation in accordance with this policy. Also, the specific IA guidelines specified in DARPA references shall be implemented within DARPA.

Scope: Basic service for all service delivery points.
Reference: SLA 33

5.3.2 Public Key Infrastructure (PKI)

Requirement: As specified in DEPSECDEF Memo dtd 09 Apr 1999, DoD PKI Implementation, any PKI employed within DoD Services and Agencies shall be the DoD PKI. Thus, the DARPA infrastructure shall incorporate DoD PKI compatibility in accordance with DoD guidelines (contained in ASD(C3I) Memorandum of 12 August 2000, Subj: DoD PKI (available from http://www.c3i.osd.mil/org/cio/doc/pki_08122000.pdf)). The contractor shall propose a PKI solution and implementation strategy for DARPA. Upon approval by DARPA, the contractor shall implement the PKI solution within DARPA. In accordance with DEPSECDEF memo dtd 10 November 1999, the primary carrier of the DoD medium assurance PKI credentials will be the Common Access Card (CAC), a smart card. The CAC will be issued by DEERS/RAPIDS to all DoD active duty military, selected reserve military, civilians, and seated contractors, DoD Total Force. CAC issuance commenced in October 2000, but distribution to DARPA personnel has yet to be scheduled. For the period of time prior to DARPA-wide deployment of the CAC, the contractor, with DARPA's approval, shall issue an alternative DoD-compliant smart card for the purposes of network logon, digital signature, etc. All PKI enabled applications in DARPA must be compatible with the DoD PKI, and authorized certificate authorities must issue all certificates. The Contractor shall perform PKI management functions, including user registration and derived key management. Specifically, the contractor shall support the following:

a. The contractor shall use only DoD-compliant PKI-enabled servers where applicable.
b. The contractor shall provide digital signature capability for all electronic mail services implemented. DoD-compliant PKI credentials will be residing on the CAC or equivalent DARPA-approved contractor-provided smart card.
c. The contractor shall register all users. This shall include registration, facilitation of the issuance of identity and email certificates (signature and confidentiality) as required (Local Registration Authority (LRA)). This shall also include management of user PKI certificates: including certificate revocation, tracking, and implementation. The registration functions shall be performed to the extent necessary to augment the DEERS/RAPIDS-LRA capability to provide all required PKI LRA and management functions for users (personnel, servers, objects, devices, etc.). The contractor shall provide user training for DoD PKI and/or DARPA-approved contractor-provided certificate use.
d. The contractor shall register servers and install server certificates for PKI enabled applications. DoD-compatible PKI certificates will be used for client-server identification and authentication for all web servers on both classified and unclassified DARPA networks.

Reference: SLA 34

5.3.3 Multi-Level Security (MLS)

Requirement: Any implementation within DARPA of a MLS device such as a High Assurance Guard or MLS Web Server shall be in accordance with the guidelines established by the Defense Information Switch Network (DISN) Security Accreditation Working Group (DSAWG) and the Secret and Below Interoperability (SABI) effort. Accordingly, in cases where the DARPA infrastructure is required to interface with other sensitive networks, such as SIPRNET, integration with an appropriate cryptographic device is required. Cryptographic devices will be provided by the government.

5.3.4 Critical Government Roles with respect to IA/CND

Although DARPA expects the Contractor to pursue an aggressive strategy for design, deployment, and operation of the DARPA infrastructure, authorized DARPA personnel must perform a number of critical security roles. These roles fall into two categories: ensuring that the security of the DARPA infrastructure satisfies DARPA, DoD, and Federal requirements and exercising essential command authority over any DARPA defensive Information Warfare (IW) activities.

The Government will furnish cryptographic equipment and keying material. The contractor shall be responsible for loading the keying material into the cryptographic equipment used to protect information classified at SECRET or below, using the Electronic Key Management System (EKMS) as appropriate. The contractor shall be accountable for all cryptographic material in accordance with the National Industrial Security Program Operating Manual (NISPOM). The contractor may be responsible for all shipping and handling of GFE DARPA cryptographic material to and from a DoD Crypto Repair Facility (CRF) for required depot repairs.

In concert with the requirements for Certification and Accreditation (C&A) of all DoD computer networks (classified and non-classified), authorized DARPA personnel under the direction of the certification authority shall be the approving authority for the following components of the DARPA infrastructure:

a. Security architecture
b. Security critical product selections
c. Network connectivity plan
d. Security procedures
e. Other security critical factors as required

In the above role, DARPA personnel will seek to use the most expeditious procedures without compromising the integrity of the security evaluation process. Also, with respect to item (b) above, the DARPA infrastructure shall comply with the National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11 for the implementation of COTS and GOTS products IA and IA-enabled IT products.

DARPA will use security assessment teams (Red and Green Teams) to conduct authorized simulated attacks against operational DARPA networks to ensure the DARPA infrastructure satisfies the security related SLAs and that DARPA, DoD, and national security requirements are adhered. As part of this approach, Red and Green Teams will also conduct design, product, and configuration reviews. The focus of Green Teams will be on contract related security requirements, while Red Teams will be less constrained and will focus on identifying vulnerabilities and risk associated with operation of the DARPA infrastructure. DARPA will ensure that DARPA, DoD, and national policies and procedures are followed in conducting Green and Red Team operations. While DARPA intends to use contractor support

personnel to supplement government personnel in conducting security assessment operations, leadership of these teams shall be government based.

With respect to CND, responses to network threats and attacks constitute Information Warfare (IW) defense command decisions that as a minimum shall be authorized by designated DARPA personnel. Along this line, the DARPA command structure shall retain directive authority over all DARPA infrastructure threat responses. These DARPA personnel shall also be the conduits for authorized responses to directives received from JTF-CND or Joint Service regional CINCs, for coordinated Joint Service response to threats. In particular, as the INFOCON level is raised, DARPA personnel shall retain command decision authority. During these periods, SLA compliance may be relaxed at the discretion of the Contracting Officer.

DARPA shall be the approving authority for the security architecture since government personnel will be responsible for security critical roles and shall have to use the infrastructure for critical operations. The security architecture is the primary mechanism that underlies the criticality of the DARPA infrastructure. The overall performance of the network shall still be the responsibility of the contractor given this constraint.

DARPA personnel will retain essential command authority and approval authority of security changes. With the constraints outlined above, the contractor is still responsible for the overall performance of the DARPA infrastructure in accordance with the SLAs.

5.3.5 Classified Information Support

The highest classification level of information that may be handled in connection with this statement of work is TOP SECRET. Since Secret data may be tunneled over the DARPA infrastructure using Type 1 encryption, the DARPA network and telecommunications infrastructures shall be required to accommodate this capability. Thus, the DARPA infrastructure shall be able to interface with Secret enclaves where required and provide a capability to transport Secret data using certified and accredited separation mechanisms such as Type 1 cryptographic products.

In accordance with the National Industrial Security Program Operating Manual, DoD 5220.M, the contractor must possess or be able to possess a Facility Security Clearance equal to the highest level of classified information necessary to perform the tasks or services required on this contract. Security requirements relating to the handling and safeguarding of classified information are identified in the DD Form 254 provided as part of the contract. Contractor personnel, whose duties require access to systems processing classified information, must possess a security clearance at least equal to the highest degree of classification involved (Top Secret) and have a validated need-to-know prior to beginning work on the classified system. All personnel who work onsite at DARPA must be cleared to the level of Secret. Currently there are approximately 5 contractor personnel onsite with Top Secret clearances.

5.3.6 Sensitive Information Support (Non-Classified)

Under current Federal guidelines, all officially held information is considered sensitive to some degree and must be protected by the contractor as specified in applicable IT Security Plans. Types of sensitive information that will be found on DARPA systems include: Privacy Act information, information that is proprietary to companies or contractors other than the subject contractor, resources protected by International Traffic in Arms Regulation (ITAR), technology restricted from foreign

dissemination, DARPA administrative communications, including those of senior Government officials, procurement and budget data, information on pending cases by Equal Employment Opportunity (EEO), labor relations, legal actions, disciplinary actions, complaints, IT security pending cases, civil and criminal investigations, and information not releasable under the Freedom of Information Act (FOIA) (e.g. payroll, personnel, and medical data).

The contractor shall perform internal assessments to determine position sensitivity and management controls necessary to prevent individuals from bypassing controls and processes, such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges at contractor facilities. These position sensitivity assessments shall be forwarded to DARPA-designated personnel for a determination of personnel suitability and requirements for individuals assigned to these positions. Periodic re-evaluations of positions and suitability requirements shall be necessary during the life of the contract as positions and assignments change.

Performance under this contract will involve access to and/or generation of sensitive information or systems. The contractor shall perform an assessment to determine position sensitivity and management controls to prevent the individuals in these positions from bypassing controls and processes such as individual accountability requirements, separation of duties, access controls, and limitations on processing privileges. Ongoing reevaluations of the position and suitability requirements will be necessary during the life of the contract as positions and assignments change.

The contractor shall conduct risk assessments, document the results, and develop and maintain internal security plans in accordance with applicable DoD guidelines and the NISPOM. These plans shall describe how the contractor will ensure the integrity, availability, and confidentiality of the information that it is operationally responsible to protect within the vendor's facilities and at government facilities. For example, the contractor shall ensure that foreign nationals within their corporate staff shall not have access to DARPA data that is not releasable per DoD security policy and the Freedom of Information Act. A decision to accept any residual risk will be the responsibility of the DARPA system owner and the DARPA information owners. The contractors risk assessments and IT Security Plans shall be updated at least every three years or upon significant change to the functionality of the assets, network connectivity, or mission of the system, whichever comes first. If new or unanticipated threats or hazards are discovered by the contractor or government, or if existing safeguards have ceased to function effectively, the contractor shall notify the government in near real time, update the risk assessments and IT Security Plans (within 30 working days) and shall make risk reduction recommendations to the DARPA system owner and the DARPA information owners (within 5 working days).

5.3.7 Privacy and Security Safeguards

The contractor shall not publish or disclose in any manner, without written consent of DARPA, the details of any security safeguards designed, developed, or implemented by the contractor under this contract.

The contractor shall develop procedures and implementation plans to ensure that IT resources leaving the control of the assigned user, such as being reassigned, removed for repair, replaced, or upgraded, is cleared of all DARPA data and sensitive application software by a technique approved by the Government, currently overwriting at least three times. For IT resources leaving DARPA use, applications acquired via a "site-license" or "server license" shall be removed. Damaged IT storage media shall be degaussed or destroyed in accordance with the NISPOM.

To the extent required to carry out a program of inspection and audit to safeguard against threats and hazards to the confidentiality, integrity, and availability of Government data, the contractor shall afford DARPA access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, databases, and personnel. DARPA will conduct an audit on an aperiodic event-driven basis the of contractor's security management processes and procedures.

5.3.8 Certification and Accreditation (C&A)

DARPA will provide the contractor with the most current information regarding the C&A status of the existing DARPA networks that comprise the "as is" configuration of the DARPA infrastructure. The contractor shall be responsible for developing a transition plan to support the migration from the "as is" DARPA infrastructure at contract award to the contractor implemented DARPA infrastructure. The contractor shall be responsible for delivering a system that can be certified and accredited in accordance with DoD Security Requirements. With this support, the contractor shall support DARPA in the following phases of C&A as defined in the DITSCAP: Definition, Verification, Validation, and Post-Accreditation. This accreditation is an essential part of the connection approval process (CAP) for SIPRNET. The contractor shall be responsible for supporting DARPA in satisfying the requirements specified in DISA MSG DTG021730Z subject DISN NON-CLASSIFIED BUT SENSITIVE INTERNET PROTOCOL ROUTER NETWORK (NIPRNET) CONNECTION APPROVAL PROCESS. Similarly, the contractor shall be responsible for supporting the Government in satisfying the DISA (DITSCAP) requirements for connection to the SIPRNET (dated 20 August 1998). This shall include providing a security concept of operations document, sufficient architecture documentation, a system security authorization agreement (SSAA), risk assessments, risk mitigation plans, and other supporting documents required to support DITSCAP accreditation. The contractor shall support DARPA in the role as certification agent.

5.3.9 DARPA Enclaves

A Community of Interest (COI) is a logical grouping of users who have a requirement to access information that should not be made available to the general DARPA user population. This requirement can be based on specific security requirements, geographical location, unique functional requirements, or unique command relationships. To meet this requirement, a logical perimeter is established around the COI, using Defense in Depth IA mechanisms. Some examples of COIs are personnel systems (for handling Privacy Act Data), geographically dispersed major claimants, and researchers and scientists handling sensitive information. COIs will be established under the authority of the DARPA Director of Management Operations (OMO).

The contractor shall dynamically establish, maintain, and disestablish multiple communities whose membership is dependent upon the presentation of community (enclave) credentials (PKI/keys), as required by and in coordination with DARPA. All of the communities above the non-classified level require Type 1 cryptographic separation. However, the DAA may authorize the use of PKI and VPN technology for COI implementation within classified enclaves. Communities within non-classified enclaves require the use of PKI and VPN technology for cryptographic separation. Connection between communities requires a Government approved gateway or guard appliance.

5.4 Catalog Services

Requirement: Catalog services shall be provided by the contractor to provide DARPA with the flexibility

to order services necessary to meet mission-essential requirements not otherwise provided as service delivery points, customer IT service, or IA/CND service. The contractor shall provide the catalog services in accordance with the requirements in the following subparagraphs:

5.4.1. COTS Catalog

COTS Catalog services provide COTS software or hardware associated with the Service Delivery Points (SDPs), or the piloting of new SDPs that may be added to support requirements beyond the basic services. (Pilot SDPs shall be understood to be SDPs obtained for testing, by the Government, the Contractor, or a Government-designated third party.) The Contractor shall provide a catalog of hardware, software and other COTS items to meet DARPA's need for specialized or advanced functionality to be ordered and funded as needed. Items listed in the catalog shall be pre-integrated and available for immediate access when ordered to augment services, or available for pilot purposes when ordered in conjunction with Expert Assistance tasks . All items in the catalog shall be integrated and interoperate with all services upon deployment. All items, except those that may function as SDPs, shall include the provision of all service identified in this SOW (i.e. installation, initial training, Help Desk, etc.) SDPs may obtain Customer IT services either through transitioning into Data Seats, or by ordering services via the Network Services Seat. Addition and removal of items from the catalog shall be upon the approval of the contracting officer representative. Items to be included in this catalog shall include but not be limited to the current non-standard but supported items listed in Attachment 2. These items shall be available for ordering through a contractor-provided, web-enabled catalog.

In the event of a COTS catalog order cancellation, the Contractor shall, in conjunction with the Government, determine if the item(s) should be returned to the original vendor or retained as an in-stock item. If the item is returned the Contractor and the Government will determine an equitable adjustment to be reflected on the Contractor's invoice. If the item is retained, its disposition will be reflected on the Credit/Asset report, and it will be available to the Government until it is fully depreciated.

Reference: SLA: 37

5.4.2 Expert Assistance Catalog

These capabilities provide labor services to support information technology-related requirements that may be needed to augment basic services or may be required beyond the basic services. The Contractor shall provide a catalog of labor categories with pre-negotiated hourly rates for DARPA to order information technology services on an as-needed basis to accommodate emerging requirements. Items available from the catalog shall be available immediately when ordered and funded. Deliverables provided under this item shall be transitionable to the basic services (i.e. installation, initial training, Help Desk, etc.) provided by this SOW if specified by DARPA. These services shall be available through a contractor-provided, web-enabled catalog. The addition and removal of labor categories from the catalog shall be upon the approval of the Contracting Officer.

Reference: SLA: 38

5.5 Transition Services

Requirement: The contractor shall provide transition services necessary to migrate current "as is" IT services to future "to be" IT services in accordance with the requirements in the following subparagraphs.

Reference: SLA to be provided as part of offeror's proposal

5.5.1 Initial Contract Transition

Requirement: The contractor shall transition assets, services and support from the incumbent contractor and DARPA staff in accordance with the transition approach incorporated by reference herein: (see offeror's proposal and DARPA's approval). In order to provide continuity of DARPA information technology services, the contractor shall assume full task order responsibility for all of the requirements in the statement of work at the beginning of the Basic period of performance, currently anticipated as (see date of full task order responsibility in offeror's proposal). During the period of (see Phase-in begin date in offeror's proposal) to (see Phase-in end date in offeror's proposal) the Contractor shall accomplish transition and training of Contractor personnel as required for the assumption of full task order responsibility. The Contractor shall not charge the Government nor be reimbursed for costs incurred for phase-in and training during said phase-in period in excess of (see cost in offeror's proposal). To ensure continuity of DARPA information technology service operations during transition and to assist the offeror in achieving successful transition, DARPA will make the incumbent contractor available for a period of time not to exceed (see number of days in offeror's proposal). To assist in transitioning explicit and tacit knowledge, methods, processes and procedures from the incumbent contractor to the successful offeror, the provisions of FAR 52.237-3(c) apply to the incumbent contractor.

Reference: SLA x (provided as part of offeror's proposal and as approved by DARPA)

5.5.2 End of Contract Transition

Requirement: In the event this contract is terminated, expires or is superseded, the contractor shall be required to turn over the items below in such a way as to facilitate a smooth, professional, business-like transition to full support by a new contractor in accordance with the provisions of FAR 52.237-3. The contractor shall perform all activities in the subparagraphs to follow, including transition planning and reporting.

5.5.2.1 Space

Requirement: The contractor shall relinquish control of all government furnished space and contractor-leased space associated solely with this contract. The contractor shall allow and facilitate the follow contractor or any other party designated by the government to transfer the lease or sub-lease the facility spaces and assume occupancy provided under this contract, whichever is more economical to the government.

5.5.2.2 Material and Services

Requirement: The contractor shall permit the government or its designee to purchase at its discretion any or all hardware, software, documentation and/or related material based on the current book value, according to the contractor's depreciation schedule, for any or all of the material in the possession of the

government in the event this contract is terminated for any reason. Likewise the contractor shall permit the government or its designee to assume any leases at it's discretion for any equipment, software, training, materials, supplies, services or communications capabilities provided under this contract in the event this contract is terminated for any reason.

5.5.2.3 Data and Files

Requirement: The contractor shall relinquish all files and documentation related to this contract, regardless of the media it is stored on (including paper, tape, diskette, CD, etc.), to the government or it's designee.

5.5.2.4 Explicit and Tacit Knowledge

Requirement: The contractor shall transition all explicit and tacit knowledge, regardless of the source or method used, including processes, procedures and methods, related to this contract to the government or its designee.

Reference: SLA x (to be provided as part of offeror's proposal)